Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:34:40 UTC

APT group: FIN8

Names	FIN8 *(FireEye)* ATK 113 *(Thales)* Syssphinx *(Symantec)* Storm-0288 *(Microsoft)* G0061 *(MITRE)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2016	
Description	(FireEye) We attribute the use of this EoP to a financially motivated threat actor. In the past year, not only have we observed this group using similar infrastructure and tactics, techniques, and procedures (TTPs), but they are also the only group we have observed to date who uses the downloader PUNCHBUGGY and POS malware PUNCHTRACK. Designed to scrape both Track 1 and Track 2 payment card data, PUNCHTRACK is loaded and executed by a highly obfuscated launcher and is never saved to disk. This actor has conducted operations on a large scale and at a rapid pace, displaying a level of operational awareness and ability to adapt their operations on the fly. These abilities, combined with targeted usage of an EoP exploit and the reconnaissance required to individually tailor phishing emails to victims, potentially speaks to the threat actors' operational maturity and sophistication. FireEye identified more than 100 organizations in North America that fell victim to this campaign.	
Observed	Sectors: Entertainment, Financial, Food and Agriculture, Healthcare, Hospitality, Retail. Countries: Canada, Italy, Panama, South Africa, USA.	
Tools used	BadHatch, BlackCat, PoSlurp, PunchBuggy, RagnarLocker, Sardonic.	
Operations performed	Mar 2016	Tailored spear-phishing campaigns In March 2016, a financially motivated threat actor launched several

		tailored spear phishing campaigns primarily targeting the retail, restaurant, and hospitality industries. The emails contained variations of Microsoft Word documents with embedded macros that, when enabled, downloaded and executed a malicious downloader that we refer to as PUNCHBUGGY. <https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html>
	2017	In early 2017, FIN8 began using environment variables paired with PowerShell's ability to receive commands via stdin (standard input) to evade detection based on process command line arguments. In the February 2017 phishing document "COMPLAINT Homer Glynn.doc" <https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html>
	Mar 2019	During the period of March to May 2019, Morphisec Labs observed a new, highly sophisticated variant of the ShellTea / PunchBuggy backdoor malware that attempted to infiltrate a number of machines within the network of a customer in the hotel-entertainment industry. It is believed that the malware was deployed as a result of several phishing attempts. <http://blog.morphisec.com/security-alert-fin8-is-back>
	Jul 2019	This blog will introduce a new reverse shell from FIN8, dubbed BADHATCH and compare publicly reported versions of ShellTea and PoSlurp to variants observed by Gigamon Applied Threat Research (ATR). <https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d:-discovering-badhatch-and-a-detailed-look-at-fin8's-tooling/>
	Mar 2021	Fin8 Group is Back in Business with Improved BADHATCH Kit <https://labs.bitdefender.com/2021/03/fin8-group-is-back-in-business-with-improved-badhatch-kit/>
	Jul 2021	FIN8 Threat Actor Spotted Once Again with New 'Sardonic' Backdoor <https://www.bitdefender.com/blog/labs/fin8-threat-actor-spotted-once-again-with-new-sardonic-backdoor/>
	Dec 2022	FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/syssphinx-fin8-backdoor>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0061/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
